PEO GCS
Information Technology & Assurance Newsletter

Issue 6 January 29, 2004

ANOTHER GREAT YEAR!

Another year has passed, but with numerous accomplishments and efforts and support being provided the PEO and PMO organizations during 2003:

- **The PEO GCS IT Support Office handled 6,241 support calls.**
- **Fielded 266 new desktop/laptop systems and 62 printers.**
- **99% Complete in the upgrading to MS 2000/XP operating systems.**
- **Upgraded server software and all wireless email devices (Blackberry's).**
- **Worked on establishing SIPRNet node in bldg 229, 3rd floor.**
- **Certified and Accredited all AIS hardware for both unclas and classified systems.**
- **Designed and successfully tested MS Sharepoint Portal system over the Detroit Arsenal Network.**
- **Received Congressional funding to expand IDE efforts throughout PEO**
- **Provided technical support to troops in Kuwait and Iraq and tested "ruggedized", but lightweight laptops in a hostile environment.**
- **Upgraded Video Bridge for multipoint VTC's for entire PEO.**
- **Procured and fielded SPAM filter for entire Detroit Arsenal**

NEW COMPUTERS

The end of the year has come-and-gone and new computers seemed to be the hot item on the menu. Your PEO GCS Support Office has been hard at work to get those new computers out of the boxes and onto your desks. The Combat Systems organization received 100 new laptops and have deployed all but a remaining few. The FCS group is not looking to shabby with 60 new laptops of their own..

Tiffany Gu is in charge of coordinating the set up of the new laptops so if she sends you an e-mail or leaves you a voice mail you may want to pay attention. Many of you returned after your last holiday or weekend to find a new laptop waiting for you already installed and ready for use. In order to make the transition to the new computers as quickly and efficiently as possible we will sometimes come in over a weekend to accomplish the task. Working on the weekend allows us to increase productivity while decreasing down-time for the customer.

We would like to thank those of you who have been patient with us in getting the new machines out over the last month and hope you are pleased with your new laptop. We look forward to working with the FCS team on our next project of getting you your new laptops as well.

NAS Conversion

Here is a topic that has affected, or will soon affect, everyone at the command. I am going to do my best to not get too technical in this article, but if I fail please just stop by our office and we will do our best to explain it in laymen's terms. I had to have it explained to me a few times before I understood it myself.

At the Detroit Arsenal we had a dual Network Operating System (NOS) network. When an individual logged into a computer he or she put in a password that authenticated them to the Novell servers and another password that authenticated them to the Microsoft servers. In most cases people made these two passwords the same so they only had to put in one and were logged in. What people may not know is that they were still logging into two servers. They just did not get prompted for the second password entry because the password was the same as the first so it was automatically accepted.

Running a dual NOS has some flaws. One of the flaws is that every 120 days you have to change your passwords and it can get confusing when you believe you only have one to change and the network is looking for two. In the last year our office has helped people with password issues over 400 times. Many of these assistance calls were not the fault of the customer, but the fault of a confusing system. The second problem is that the network runs slower when you have two NOS' running on it. Network traffic is not handled smoothly and it becomes very difficult to get a good handle on what is causing a dilemma, or where a bottleneck may be slowing everyone down. Lastly the Novell servers, which are the file servers we are used to hearing about (PEOGCSS, TARDEC1, IMMC1, ACQ…), are out-of-date and can no longer handle the storage requirements of the work force. The area of the PEOGCSS server that we all shared for our home drives and share drives was only 40 Gigabytes, or about the size of standard laptop hard drives these days.

To resolve these issues all accounts on the PEOGCSS server were moved to a server called the NAS (Network Attached Storage).

The NAS is a server that uses Microsoft 2000 Server Professional and will be upgraded to Microsoft 2003 Server this year. It has more than 10 times the storage capacity of all of the Novell servers at the Detroit Arsenal combined. Since it is using Microsoft software it is also compatible with the new Army standard.

As well as housing our home and share drives the Novell servers managed all of our network printers. In preparation for the move our team attempted to get every single network printer moved over to the NAS. Share and home drives are also handled differently on the NAS. Data in your home drive is still only visible to you. Data in your share drive is now visible to everyone at the command, but with the owner only having the rights to modify, create, or delete data in your share drive. Your share and home drives also have been increased to a limit of 100 megabytes. Some people were using their share drives as a community storage area for documents. On the NAS this will not work. For those of you that require an area for sharing documents quickly and efficiently you will notice a T: drive now shows up under My Computer. This is the Team Folders area and is designated for sharing documents with others. If you would like to set up a Team Folder just send a request to PEOGCS SUPPORT and let us know what you would like the name of the folder to be, who you want to have rights to the folder, and what rights you would like these people to have (i.e. read, write, modify, delete).

We are coming to the end of the transition phase of this move and appreciate your understanding and patience. If you have any questions regarding the migration to the NAS please feel free to stop by our office, give us a call (47469), or send us an e-mail at PEOGCS SUPPORT.

AKO

In support of Army Security requirements, AKO requires the use of browsers that support 128 bit encryption Browsers that do not support this level of security will not be able to access AKO. Current versions of Internet Explorer and Netscape support 128 bit encryption, and can be downloaded from vendor sites (http://www.Microsoft.com for Internet Explorer or http://www.Netscape.com for Netscape). Please call the AKO Help Desk at 877-AKO-USER if you have any questions

Portal

The PEOGCS CIO Army Knowledge Management team will be deploying the newest of Microsoft's Share Point Portal server 2003 early this year. Share Point Portal Server 2003 lets you experience full object oriented functionality, including news; sites directory; topic areas; personal sites (My Portal); audience targeting; easy search and browsing capabilities to help users find people, teams, and information; and site provisioning to provide the necessary structure to create connected collaboration spaces. Organizations and users will be able to retrieve, collaborate, store, and discuss their day-to-day business documents in a tailorable and scaleable environment.

Personal sites (My Portal).

My Portal has a private view so that users are able to develop and work in a user specific/defined environment, enabling the user to store and access personal content securely, such as unfinished documents, customized reference areas, or links to webified systems specific to their needs. The tailoring of My Portal is for the individual user, for example a finance person can configure the environment to their needs, a procurement person can configure their environment to what matters to them, and so on.   So instead of having to log into and out of one website and into another, a user can have multiple sites open for their use. Think of it, on your personalized portal environment you can have your email open, be logged into the AKO, and an Army financial system, and know the weather in Washington, DC….all on one screen. In addition My Portal also has a "public" feature that allows individual users to establish a personal web site of sorts for access by all users with account in the PEO GCS eBusiness environment. The users can also develop a public view that enables users to publish content such as presentations and finished reports to other users…like a personal web site!

Single sign-on with AKO

Single sign-on (SSO) enables users to access secure data throughout the enterprise with a single login. Share Point Portal Server securely stores account credentials when users sign on to the portal. The PEO-GCS Knowledge Management Team is currently working with SSO software manufacturer Netegrity to provide SSO while logged in from the Army Knowledge Online website.

Search

Share Point Portal Server 2003 enables users to search full document text and properties for the keywords that they enter. Not only can users search for information, but they can browse and search for people, teams, and other sites on the portal.

INFORMATION ASSURANCE HEADLINES

Threat: Non-DoD individuals attempting to gain access to Army networks. An AKO user received an unsolicited email stating that their user ID and password were compromised. The unsolicited email stated the AKO user should visit a website (no information provided) and input their old user ID and password to gain a new user ID and password. At the risk of being tediously monotonous, beware! Under no circumstances will users provide their account user ID and password to anyone. If you receive an email/phone call stating you should provide your user ID and password because there is a problem with it, you should report that to your Information Assurance Security Officer (IASO) immediately. Never share your user ID and password with anyone.

Policy Reminder, Stickers: Many personnel have been receiving new work stations and/or laptop computers over the past few months. All computer equipment and components and other devices used for data processing, copying, scanning and so on, must bear a label identifying the highest level of processing authorized. Since most workstations are used for unclassified processing up to the Sensitive but Unclassified (SBU) level, most should have a green label stating "THIS MACHINE IS AUTHORIZED FOR PROCESSING SBU DATA". Fully unclassified machines will have a blue label, a red label for machines authorized up to and including Secret, and a yellow label for Top Secret. If your machine is not labeled, please notify your IASO immediately! A DA inspection team will be in the area in the near future, and will be observing such discrepancies. IASOs and Systems Administrators should check through their areas and personally label all equipment that is currently unlabeled or improperly labeled.

Another Policy Reminder, Screen Savers: This may be becoming old and monotonously boring, but there are still numerous individuals throughout the PEO who are not utilizing screen savers. Every PC, be it a desktop, laptop, notebook or whatever you want to call it, MUST have the screen saver enabled and password protected. Recent Detroit Arsenal policy has dictated a setting of three (3) minutes. However, PC's being "imaged" by the Detroit Arsenal DOIM are returning with a default setting of ten (10) minutes, which cannot be changed on an imaged machine. Therefore, any setting of between three and ten minutes is acceptable. If you don't know how to turn on your screen saver, contact your IASO or the Tech Support team.

Just Good Sense: Here are some useful tidbits of information that are intended to enhance the overall and individual security posture at home as well as away.

a. ***Password protect your Blackberry.*** If you have been issued a Blackberry device, sit down right now, go into "Options" and then "Security" and put in a password. You can also set the security timeout - how long the Blackberry will remain idle before locking and requiring your password to re-access - in the Security window. The default is two (2) minutes, which is recommended. If you lose your Blackberry and it is not password protected, the finder (or thief, as the case may be) has access to all your files, and can even send e-mail in your name! This is considered a Security Incident and could result in disciplinary action. However, if you have set a password and then lose the device, several attempts to "guess" your password will result in the device being completely reset and all files erased! Now that's good security!

b. ***Slow down and look around.*** Many individuals have returned from travel short an item or two that they left with. If that item happens to be Government Property, then we may have a problem. The most frequent "forgotten" item is a power unit for a laptop. Other items left behind have included phone cords, mice, Blackberry devices, and even a cellular telephone. The more expensive of these items - such as the power supply, Blackberry and CelTel, can result in the need of a report of survey and you the individual having to reimburse the Government for the loss. Try to slow down a little and not rush out the door of your hotel room. Make a thorough check of the complete room before you leave, including drawers, closets and under the bed. If using equipment in the airport or somewhere else in a waiting status, keep aware of announcements regarding flight information or whatever it is you are waiting on. That will prevent hearing that "final boarding call" resulting in you jumping up and rushing to the gate, leaving your Blackberry on the seat behind you. To employ an old adage: Haste makes waste!

c. ***Who's that behind you?*** Given the security situation around the world these days, especially for Americans, it pays to be extra observant. No matter where you are, always keep a look around you noting individuals near you and not-so-near or, if driving, vehicles around you and their drivers/passengers. When driving, your efforts should be directed fully towards driving, not talking on the phone or doing other things that distract your full attention from the road. Use that full attention to keep aware of who is in your mirrors, next to or in front of you. This is especially important when outside the U.S. In airports, train stations, on buses, or wherever, just try to be aware of those around you, especially ones who seem to be around you a little too frequently. Report any suspicious activities to local authorities and/or to your Security Officer upon your return. Just a friendly OPSEC reminder.

Spam: If you've been bothered with more SPAM (unsolicited email and advertisements) lately, there is nothing to be alarmed about. The DOIM has recently undergone a change of contractors regarding the external e-mail gateways into Detroit Arsenal. The outgoing contractor took his email filtering with him. PEO GCS has recently funded the DOIM to install a new SPAM filter called "Ironmail", scheduled for the not-too-distant future. The software and hardware have been ordered and will require some testing before being fully deployed on the network. In the meantime, you can use your Outlook junk mail capabilities to cut down on SPAM and do some filtering of your own. Contact the Tech Support staff for assistance in activating that function.

Certification and Accreditation:

(1) The APEO CI Office has begun the process to accredit all AIS equipment and software within the organization. This effort will encompass more than 600 users and over 1000 pieces of equipment, to include desktops, laptops, wireless devices, printers, routers, hubs, etc. We plan on completing this effort by Dec 15th, with final reports and summation documentation being completed before the end of the year.

(2) The PEOGCS CIO standard operating procedure for the Defense Information Technology Certification and Accreditation Program (DITSCAP) is undergoing updates and changes, and will be circulated for review again very soon. The changes are a result of changes (personnel and structure) within the PEO, as well as in the way some PM's are handling C&A requirements. If you are involved in the C&A process, are an IASO, PM or Systems Administrator, you should review the SOP and comment as you see fit.

NEW EMPLOYEE DAVE OLESON

In an effort to keep up the high quality of support we offer for our PEO GCS customers we have added a team member. Late last year Dave Oleson started work with our team. Dave is joining us from Florida where he worked at Ft. Tyndall . His previous job requirements and work atmosphere were extremely similar to what our office deals with here and he is fitting in wonderfully. While we won't hold it against him, before that Dave spent 20 years in the Navy. To answer that question which everyone has at this point, "Why would you move from Florida to Michigan?" Dave's wife recently retired from the Navy and she wanted to move back to where she grew up, Michigan. What a great husband.